# TAB F

THE SEDONA CONFERENCE℠ WORKING GROUP SERIES

wgs℠

# THE SEDONA GUIDELINES:

## *Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*

A Project of The Sedona Conference℠
Working Group on
Best Practices for Electronic Document
Retention & Production

September 2004 Public Comment Draft

> process that resulted in the patented invention. PatentCo's records management policy and retention schedule requires that laboratory notebooks be kept permanently so that it can re-create the inventive process if necessary. When patent litigation occurs later, PatentCo is able to show that it filed its patent application less than one year from the date of its scientist's discovery of a successful process, avoiding a claim that its patent is invalid.

The value of information will vary greatly from organization to organization, and even within an organization. How an organization chooses to capture this value may also vary accordingly. One organization may choose to concentrate its resources on capturing the value in its research or product development records while another may emphasize its sales or marketing resources. The solutions, policies, practices and training employed, as well as the technological resources invested, will reflect internal business judgments as to the best approach for that entity. This makes it impossible to develop a "generic" information and records management policy appropriate for every organization. *See* Comment 1.c, *supra.* Organizations should make a conscious effort to recognize and make accessible the information necessary to meet the organization's needs and responsibilities. Conversely, information not of value may and should be discarded, *see* Guideline 3, subject, of course, to the need to preserve all discoverable information needed for litigation purposes. *See* Guideline 5.

**Comment 2.e.**

**A business continuation or disaster recovery plan has different purposes from those of an information and records management program.**

Business continuation or disaster recovery plans and programs, such as those employing backup systems, allow an organization to rebuild its electronic information systems and to continue operations despite a significant network failure. *Cf.* Marianne Swanson et al., NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS (2002). What must be stored in order to achieve this goal and the manner and length of storage time will generally be decided by an organization's information technology professionals (with substantive input from the other disciplines—operational, records management and legal) as the individuals who will be relied on to manage the recovery. Consideration should typically be given to making the storage time period as short as possible—only that amount of time that is truly necessary to recover from a disaster.

There is general consensus that regardless of the various capabilities of different backup systems, those systems are designed for the purpose of business continuity and should not be used as a substitute for records management. While the back-up systems can provide critical capabilities to recover data when necessary, those capabilities are fundamentally different from what is required for information and records management. Moreover, after a relatively short period of time, it is simply impractical for back up systems to retrieve efficiently or effectively specific, targeted information. Accordingly, it would be useful and reasonable to reflect this in the policies, procedures and programs by separately providing for disaster recovery systems and procedures applying to electronic information and records management.

The policy for disaster recovery for electronic information should describe:

- What constitutes a "disaster" requiring information restoration;

### 3. An organization need not retain all electronic information ever generated or received.

**Comment 3.a.**

**Destruction[1] is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.**

At the heart of a reasonable information and records management approach is the concept of the "lifecycle" of information based on its inherent value. In essence, this means that information and records should be retained only so long as they have value as defined by business need or legal requirement. Thus, while some documents contain information which is deemed irreplaceable and must be indefinitely retained (or "archived"), information and records that do not have such continuing value to the organization can be destroyed or deleted when the organization, in its business judgment, determines it is no longer needed, regardless of the form (*i.e.*, paper or electronic). Of course, this destruction in the ordinary course is subject to suspension when there is actual or reasonably anticipated litigation. *See* Guideline 5 and commentary; *see also The Sedona Principles: Best Practices, Recommendations, and Principles for Addressing Electronic Document Production*, Principle No. 5 (Jan. 2004) ("The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.") and associated commentary.[2]

Retaining superfluous electronic information[3] has associated direct and indirect costs and burden that go well beyond the cost of additional electronic storage. The direct costs include additional disk space, bandwidth, hardware, software, archival systems and the cost of their related media migration requirements and possibly even storage area networks to store such information. The cost of storage alone can be significant, particularly where minimum standards exist concerning the storage media for such information.[4]

The indirect costs include the cost of technical staff for maintaining such information, the cost of personnel classifying such information, and the potential cost of outside counsel to review and exclude irrelevant electronic information in the discovery process.

There is no question that managing unneeded information increases an organization's costs, burdens, and ability to fashion an adequate and timely defense in litigation. For example, irrelevant electronic information can hamper efforts to locate and produce information or records that are requested in litigation. This can lead to substantial monetary sanctions when required records or information are not timely produced. An organization can control these costs by identifying information of value to it, and reducing the amount of irrelevant electronic information that it

---

[1] We use the word "destruction" so there is no ambiguity. An organization, in drafting its policy, may use different terminology.

[2] It is important to note that not all threatened litigation or conceivable disputes will trigger preservation obligations. The analysis, however, must be done on a case-by-case basis and organizations should be prepared to analyze such situations as they arise. *See* Guideline 5.

[3] If it is superfluous (*i.e.*, unnecessary), it would, by definition, not have even marginal value.

[4] *See* ANSI standards for storage of magnetic and digital information, which include monitoring of temperature and humidity levels, physical security, magnetic field restrictions, acceptable fire retardants, exercising magnetic tape to prevent stiction, etc.

retains. *See Smith v. Texaco, Inc.*, 951 F. Supp. 109, 112 (E.D. Tex. 1997), *rev'd on other grounds*, 263 F. 3d 394 (5th Cir. 2001) (court upheld temporary restraining order prohibiting defendants from altering or destroying documents related to employment discrimination litigation; however, given the high cost of electronic storage, court permitted deletion of electronic documents in the ordinary course of business so long as hard copies were kept).

Managing superfluous information does not merely result in unnecessary costs. It also drains an organization's limited internal and external human and material resources. It diverts the organization's internal resources from advancing the organization's principal business objectives of efficiency and productivity. It diminishes the organization's ability to compete in the marketplace, while unduly increasing the cost of doing business. Dealing with the issues that can arise from having too much information in litigation can also divert the attention of an organization's outside counsel from the strategic and substantive issues to matters of discovery and process.

Courts routinely acknowledge that organizations have the "right" to destroy (or not track or capture, whether or not it is consciously deleted) electronic information that does not meet the internal criteria of information or records requiring retention. *See McGuire v. Acufex Microsurgical, Inc.*, 175 F.R.D. 149, 155-56 (D. Mass. 1997) (in the employment context, while there is no broad right to "broom clean" internal investigation files or edit personnel records "willy-nilly," employers may call for and edit drafts, and discard them where there are errors made by someone other than the accuser; "to hold otherwise would create a new set of affirmative obligations for employers, unheard of in the law—to preserve all drafts of internal memos, perhaps even to record everything no matter how central to the investigation, or gratuitous"); *cf. United States v. Arthur Andersen, LLP*, ___ F.3d ___, 2004 WL 1344957, at *11 (5th Cir. June 16, 2004) ( "A routine document retention policy, for example, evidences an intent to prevent a document from being available in any proceeding. But it does not alone evidence an intent to "subvert, undermine, or impede" an official proceeding."); *Stevenson v. Union Pac. R.R.*, 354 F.3d 739, 748-49 (8th Cir. 2004) (recognizing legitimate aspects of a retention program that resulted in the destruction of materials). *But see Morris v. Union Pac. R.R.*, 373 F.3d 896 at 900-01 (8th Cir. 2004) (holding that adverse inference instruction sanction for destruction of engineer-dispatcher audiotape made at the time of accident was improper, distinguishing facts in *Stevenson*).

It should be noted, however, that deciding not to track or capture electronic information does not render it immune from discovery should litigation ensue. An organization may thus reduce the amount of superfluous electronic information that it retains even where litigation is involved, provided that its preservation obligations are met.

> ***Illustration i.*** Company A, which does not have an automated program to enforce e-mail retention and disposition, collects 1 million pages in e-mail and associated attachments from 25 employees in preparing a response to a government investigation. All pages are data converted and scanned at a cost of $0.20/page, a total of $200,000. A team of attorneys reviews the collection for relevance to the request and for privilege determinations at a cost of $0.50/page, $500,000 total. Upon completion of the culling process it is found that 10%, or 100,000 pages were responsive to the request. Company A has spent $700,000 to produce 100,000 pages. It is safe to estimate that between 50–75% of the records retained in the employee's e-mail accounts did not have "retention value." Therefore,